Michael Kind
Mk@kindlaw.com
KIND LAW FIRM
8860 S. Maryland Parkway, Suite 106
Las Vegas, NV 89123
Tel.: (702) 337-2322
(702) 329-5881 (fax)

Gayle M. Blatt, (*pro hac vice forthcoming*)
gmb@cglaw.com
CASEY GERRY SCHENK
FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Tel: (619) 238-1811; Fax: (619) 544-9232

Attorneys for Plaintiff and the Putative Class
[Additional Counsel on Singnature Page]

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

RONALD STALLONE, on behalf of himself and all other persons similarly situated,

Plaintiff,

v.

FARMERS GROUP, INC., a Nevada Corporation; FARMERS INSURANCE EXCHANGE; and TRUCK INSURANCE EXCHANGE,

Defendants.

Case No.

CLASS ACTION COMPLAINT

Demand for Jury Trial

Plaintiff Ronald Stallone, individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to him and on information and belief as to all other matters, by and through undersigned counsel, hereby brings this Class Action Complaint against Defendants Farmers Group, Inc.; Farmers Insurance Exchange; and Truck Insurance Exchange (collectively "Farmers" or "Defendants"), and alleges as follows:

INTRODUCTION

1. Every year millions of Americans have their most valuable personal information stolen and sold online because of unauthorized data disclosures. Despite the dire warnings about the severe impact of unauthorized data disclosures on Americans of all economic strata, companies still fail to put adequate security measures in place to prevent the unauthorized disclosure of private data about their customers or potential customers.

2. Defendants Farmers Group, Inc., Farmers Insurance Exchange, and Truck Insurance Exchange provide insurance products, including car insurance, to Americans across the country. As a part of that business, Defendants collect and provide sensitive personal information about members of the public when customers or potential customers request a quote for Defendants' car insurance products. And they do this while promising they "value your privacy" and that "[o]ur policy is to protect the confidentiality of the individually identifiable information . . . and to limit access to that information only to those with a need to know."[1]

3. Defendants failed to meet their promises and obligations to protect personal information. Defendants readily provided Plaintiff's and putative Class Members' driver's license numbers to literally *anyone* who entered a person's name, address and/or date of birth into their on–line quoting system. Thus, customers, prospective customers, and even members of the public, like Plaintiff, who were not

[1] https://www.farmers.com/privacy-statement/ (last visited June 10, 2021).

even prospective customers of Defendants, had this sensitive personal information compromised and essentially made available to the public.

4. As reported by Defendants, between January 20, 2021, and February 12, 2021, "unknown malicious actors targeted the Farmers Auto quoting system to obtain various individuals' personal information."[2] Defendants state they are still investigating "exactly how this occurred." But, at a minimum, between at least January 20, 2021, and February 12, 2021, Plaintiff's and Class Members' driver's license numbers were stolen by malicious actors.

5. Because Defendants access and store personal information—including driver's license numbers—from motor vehicle records as defined by the Drivers' Privacy Protection Act, Defendants are legally required to protect personal information ("PI") from unauthorized access and exfiltration.

6. As a result of Defendants' failure to provide reasonable and adequate data security, Plaintiff's and the Class Members' PI has been exposed to, and stolen by, those who should not have access to it. Plaintiff and the Class are now at much higher risk of identity theft and for cybercrimes of all kinds, especially considering the highly valuable and sought–after PI stolen here.

THE PARTIES

7. Plaintiff Ronald Stallone is a resident of Hicksville, New York. In or about April 2021, he received notice from Defendants that they improperly exposed his driver's license number to an unknown third party. Yet, Plaintiff Stallone never even sought a quote for insurance from Defendants. In or about May 2021, Plaintiff Stallone received a letter stating that his application for credit at Eddie Bauer was not approved. Plaintiff Stallone never applied for credit at Eddie Bauer.

8. Defendant Farmers Group, Inc., is a Nevada corporation with its principal place of business in Woodland Hills, California. Farmers is the

[2] https://oag.ca.gov/system/files/Breach%20notice%20CA-FFQ.pdf (last visited August 9, 2021).

management company ("attorney–in–fact") hired by Defendants Farmers Insurance Exchange and Truck Insurance Exchange to conduct business on behalf of policy holders throughout the United States.

9. Defendant Farmers Insurance Exchange is a California company, with its principal place of business in Woodland Hills, California. Farmers Insurance Exchange is an inter–insurance exchange organized under California Insurance Code section 1300, *et seq.*, and provides insurance throughout the United States.

10. Defendant Truck Insurance Exchange is a California company, with its principal place of business in Woodland Hills, California. Truck Insurance Exchange is an inter–insurance exchange organized under California Insurance Code section 1300, *et seq.*, and provides insurance throughout the United States.

11. Defendants, collectively, operate as a single unincorporated business enterprise selling insurance under the service mark "Farmers Insurance Group of Companies."[3] Defendant Farmers Group, Inc. operates as the attorney–in–fact for the collective, and provides management services and handles the business functions of the Defendants Farmers Insurance Exchange and Truck Insurance Exchange—except for claims processing. The business services include supplying employees; underwriting, accounting, and actuarial services; investment advice and services, facilities and equipment purchasing, and computer systems.

12. Plaintiff alleges that each Defendant acted in all respects pertinent to this action as the agent of the other Defendants, carried out a joint scheme, business plan or policy in all respects pertinent hereto, and the acts of each Defendant are legally attributable to the other Defendants. The actions of each Defendant alleged in this complaint were ratified and approved by the officers and/or managing agents of every other Defendant.

[3] United States Patent and Trademark Office, Registration Number 1821672

JURISDICTION AND VENUE

13. The Court has federal question jurisdiction under 28 U.S.C. § 1331 for the Drivers' Privacy Protection Act claims and supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367. Also, subject matter jurisdiction in this civil action is authorized pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class Members, at least one class member is a citizen of a state different from that of Defendants, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

14. This Court has personal jurisdiction over Defendant Farmers Group, Inc. because it is incorporated in Nevada.

15. This Court has personal jurisdiction over Defendant Farmers Insurance Exchange because, based on information and belief, it solicits and conducts substantial business in Nevada.

16. This Court has personal jurisdiction over Defendant Truck Insurance Exchange because, based on information and belief, it solicits and conducts substantial business in Nevada.

17. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant Farmers Group, Inc. is incorporated and resides in this District, and on information and belief, a substantial part of the events or omissions giving rise to Plaintiff's and Class Members' claims occurred in this District.

FACTUAL ALLEGATIONS

A. Defendants collect PI and fail to provide adequate data security.

18. Defendants provide insurance and are "proud to serve more than 10 million households with more than 19 million individual policies across all 50 states . . . ."[4]

[4] https://www.farmers.com/about-us/ (last visited August 9, 2021).

19. Defendants offer a public–facing insurance quoting platform for visitors on their website. Visitors to their website can receive a quote for auto insurance after providing personal information.

20. Defendants' quoting feature uses the information entered by the website's visitor and combines it with additional information Defendants collect from consumer reporting agencies, including driving records, driver's license numbers, and loss history reports, to provide the visitor a quote for car insurance.

21. In and around January-February 2021, Defendants' instant insurance quote feature was used by unauthorized third parties to obtain Plaintiff's and Class Members' drivers' license numbers ("Unauthorized Data Disclosure"). This was made possible by Defendants' failure to properly secure their instant quote system, allowing anyone with basic information to obtain drivers' license numbers and other sensitive data.

22. Defendants' failure is even more egregious because Defendants published an article acknowledging the importance of computer security and promoting the use of penetration testing in June 2019—a year and half before the Unauthorized Data Disclosure.[5]

23. Following the Unauthorized Data Disclosure, Plaintiff received a letter from Defendants entitled "Notice of Data Breach," dated April 22, 2021. The letter stated that his PI may have been compromised, including his drivers' license number.

24. In or about May 2021, Plaintiff Stallone received a letter stating that his application for credit at Eddie Bauer was not approved. Plaintiff Stallone never applied for credit at Eddie Bauer.

25. After receiving such letters, and because of the substantial and imminent risk of future harm (including identity theft) to which Plaintiff and Class Members

[5] https://www.farmers.com/learn/plan-and-prep/phishing-scams-and-other-high-tech-mischief/ (Last visited August 20, 2021.)

are now subject, Plaintiff and the Class members must take steps to mitigate that substantial risk of future harm. In fact, in Farmers' letter it encourages affected individuals to use the identity theft protection service it offers to Plaintiff and Class Members to help protect their identity from misuse, and that they should, "[i]n addition to enrolling in Credit Monitoring . . . order your free credit report, place a fraud alert on your credit bureau file, place a security freeze on your credit file and report suspicious activity."

B. The PI exposed because of Defendants' inadequate data security is highly valuable on the black market.

26. The information exposed by Farmers is very valuable to phishers, hackers, identity thieves and cyber criminals, especially at this time where unprecedented numbers of fraudsters are filing fraudulent unemployment benefit claims.

27. Cybercrime has been on the rise for the past decade and continues to climb exponentially; as of 2013 it was being reported that nearly one–out–of–four data breach notification recipients become a victim of identity fraud.[6] Defendants fully aware data security breaches are increasing, and even offer Cyber Liability and Data Security program aimed to protect businesses.[7]

28. Stolen PI is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

[6] Pascual, Al, "2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters," *Javelin* (Feb. 20, 2013).

[7] https://finance.yahoo.com/news/farmers-insurance-offers-cyber-liability-180925281.html (Last visited August 20, 2021.)

29. When malicious actors infiltrate companies and copy and exfiltrate the PI those companies store, or have access to, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[8]

30. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings—many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now–defunct AlphaBay,

> are awash with [PI] belonging to victims from countries all over the world. One of the key challenges of protecting [PI] online is its pervasiveness. As data disclosures in the news continue to show, [PI] about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target.[9]

31. The PI of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[10] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[11]

---

[8] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28, 2020, *available at:* https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited June 10, 2021).

[9] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, *available at:* https://www.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited May 29, 2021).

[10] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited May 29, 2021).

[11] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-

32. The information compromised in the Unauthorized Data Disclosure is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Unauthorized Data Disclosure is difficult, and highly problematic, to change—driver's licenses and addresses.

33. Recently, Forbes writer Lee Mathews reported on Geico's similar data disclosure wherein hackers also targeted driver's license numbers, "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[12]

34. National credit reporting company, Experian, blogger Sue Poremba also emphasized the value of driver's license to thieves and cautioned:

> If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license is one of the most important pieces to keep safe from thieves.[13]

experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited May 29, 2021).

[12] Lee Mathews, *Hackers Stole Customers' License Numbers from Geico in Months-Long Breach*, (April 20, 2021), *available at*: https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3066c2218658 (last visited May 29, 2021).

[13] Sue Poremba, *What should I do If My Driver's License Number is Stolen?* (Oct. 24, 2018), *available at*: https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last visited May 29, 2021).

35. In fact, according to CPO Magazine, which specializes in news, insights, and resources for data protection, privacy, and cyber security professionals, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation." Tim Sadler, CEO of email security firm Tessian, points out why this is not the case and why these numbers are very much sought after by cyber criminals:

> It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks. . . . bad actors may be using these driver's license numbers to fraudulently apply for unemployment benefits in someone else's name, a scam proving especially lucrative for hackers as unemployment numbers continue to soar. . . . In other cases, a scam using these driver's license numbers could look like an email that impersonates the DMV, requesting the person verify their driver's license number, car registration or insurance information, and then inserting a malicious link or attachment into the email.

36. Drivers' license numbers have been taken from auto–insurance providers by hackers in other circumstances, indicating both that this specific form of PI is in high demand and also that Farmers knew or had reason to know that their security practices were of particular importance to safeguard consumer data.[14]

37. Once PI is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax

[14] *See* United States Securities and Exchange Commission Form 8-K for INSU Acquisition Corp. II (Feb. 1, 2021), https://www.sec.gov/Archives/edgar/data/1819035/000121390021005784/ea134248-8k_insuacquis2.htm?=1819035-01022021 (accessed Apr. 27, 2021) (announcing a merger with auto-insurance company MetroMile, Inc., an auto-insurer, which announced a drivers' license number Data Disclosure on January 19, 2021); Ron Lieber, *How Identity Thieves Took My Wife for a Ride*, N.Y. TIMES (Apr. 27, 2021) (describing a scam involving drivers' license numbers and Progressive Insurance).

details. This can lead to additional PI being harvested from the victim, as well as PI from family, friends, and colleagues of the original victim.

38. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet–enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

39. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendants did not rapidly report to Plaintiff and Class Members that their PI had been stolen. It took Farmers over two months to do so.

40. Victims of drivers' license number theft also often suffer unemployment benefit fraud, harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

41. Unauthorized data disclosures facilitate identity theft as hackers obtain consumers' PI and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PI to others who do the same.

C. Defendants were on notice of the sensitivity and private nature of the PI it utilized for insurance quotes and their duty to safeguard it.

42. "Insurance companies are desirable targets for cyber attackers because they work with sensitive data."[15] In fact, according to the Verizon 2020 Data Breach Investigations Report there were 448 confirmed data breaches in the financial and insurance industries.[16]

[15] Data Protection Compliance for the Insurance Industry (October 7, 2020), *available at*: https://www.ekransystem.com/en/blog/data-protection-compliance-insurance-industry (last visited May 29, 2021).

[16] Verizon 2020 Data Breach Investigations Report (2020), available at: https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf (last visited May 29, 2021).

43. Defendants claim they:

> are committed to properly safeguarding consumer personal information and only using data in a manner that is necessary for servicing or better understanding our customers or potential customers. Our policy is to protect the confidentiality of the personally identifiable information that you provide, and to limit access to that information only to those with a need to know.[17]

44. Defendants' Privacy Policy also notes:

> that if state law is more protective of an individual's privacy than federal privacy law, we will protect information in accordance with state law while also meeting federal requirements." Further, they state "[p]rotecting your privacy is important to us. We maintain physical, electronic, and procedural safeguards that comply with applicable regulatory standards to guard your nonpublic personal information. We do not disclose any nonpublic personal information about you except as described in this notice or as otherwise required or permitted by applicable law.[18]

45. Defendants claim they "maintain[] physical, electronic, and procedural safeguards,"[19] however, those safety and security measures were insufficient. And while Defendants state the information is protected by safeguards, it was not. The weakness in Defendants' systems allowed access to, and the exfiltration of, Plaintiff's and the Class Members' driver's license numbers.

D. Farmers failed to comply with Federal Trade Commission requirements.

46. Federal and State governments have established security standards and issued recommendations to minimize unauthorized data disclosures and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses highlighting the importance of

[17] https://www.farmers.com/privacy-center/ (last visited June 10, 2021).
[18] https://www.farmers.com/content/dam/falcon/pdf/privacy-center/Farmers-Privacy-Notice.pdf (last visited June 13, 2021).
[19] https://www.farmers.com/content/dam/falcon/pdf/privacy-center/Farmers-Privacy-Notice.pdf (last visited June 10, 2021).

reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision–making.[20]

47. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, establishing guidelines for fundamental data security principles and practices for business.[21] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[22]

48. The FTC also recommends companies limit access to sensitive data; require complex passwords to be used on networks; use industry–tested methods for security; monitor for suspicious activity on the network; and verify third–party service providers have implemented reasonable security measures.[23]

49. Highlighting the importance of protecting against unauthorized data disclosures, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PI, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal

[20] *See* Federal Trade Commission, *Start With Security* (June 2015), available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited May 29, 2021).
[21] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited May 29, 2021).
[22] *Id.*
[23] Federal Trade Commission, *Start With Security*, *supra* footnote 25.

Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[24]

50. Through negligence in securing Plaintiff's and Class Members' PI and allowing anyone to utilize their instant quote website platform to obtain access, view, and exfiltrate individuals' PI, Farmers failed to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and the Class Members' PI. Farmers' data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

E. Plaintiff Stallone's attempts to secure his PI after the breach.

51. In or about April 2021, Plaintiff Stallone received a notice from Farmers dated April 22, 2021("Notice Letter"), informing him of the Unauthorized Data Disclosure and that his driver's license number may have been accessed.

52. Following the Unauthorized Data Disclosure, Plaintiff Stallone received a letter dated May 25, 2021, denying his application for credit at Eddie Bauer. However, Plaintiff Stallone never applied for credit at Eddie Bauer.

53. Following receipt of the Notice Letter and learning of the denial of Eddie Bauer credit, Plaintiff Stallone made reasonable efforts to mitigate further impact of the Data Breach, including reviewing and monitoring his accounts, enrolling in the free credit monitoring offered, and placing an alert on his credit with Experian.

54. Plaintiff Stallone researched his options to respond to the theft of his driver's license. He spent, and continues to spend, additional time reviewing his credit monitoring service results and reports from other online resources concerning the security of his identity and financial information. This is time Plaintiff Stallone

[24] Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, available at https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Jan. 8, 2021).

otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life.

55. Plaintiff Stallone has never knowingly transmitted unencrypted PI over the internet or any other unsecured source. He deletes any and all electronic documents containing his PI and destroys any documents that contain any of his PI, or that may contain any information that could otherwise be used to compromise his PI.

56. Plaintiff Stallone suffered actual injury from having his PI exposed because of the Unauthorized Data Disclosure, including, but not limited to: (a) identity theft or fraud; (b) loss of his privacy and control over his use of his PI; and (c) imminent and impending further injury arising from the increased risk of fraud and identity theft.

57. As a result of the Unauthorized Data Disclosure, Plaintiff Stallone was a victim of identity theft, and will continue to be at heightened risk for financial fraud, future identity theft, other forms of fraud, and the attendant damages, for years to come.

F. Plaintiff and Class Members suffered damages.

58. Plaintiff and Class Members are, and will continue to be, at risk for actual identity theft in addition to all other forms of fraud.

59. The ramifications of Farmers' failure to keep individuals' PI secure are long lasting and severe. Once PI is stolen, fraudulent use of that information and damage to victims may continue for years.[25]

60. The PI belonging to Plaintiff and Class Members, respectively, is private, valuable, and sensitive in nature as it can be used to commit a lot of different harms in the hands of the wrong people. Defendants failed to obtain Plaintiff's and Class

[25] *2014 LexisNexis True Cost of Fraud Study*, (August 2014), *available at*: https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last visited May 29, 2021).

Members' consent to disclose such PI to any other person as required by applicable law and industry standards.

61. Farmers' inattention to the possibility that anyone, especially thieves, with various pieces of individuals' data, could obtain any individual's PI by engaging with their front–facing instant quote platform left Plaintiff and Class Members with no ability to protect their sensitive and private information.

62. Farmers had the resources necessary to prevent the Unauthorized Data Disclosure, but neglected to adequately implement data security measures, despite their obligations to protect PI of the Plaintiff and Class Members from unauthorized disclosure.

63. Had Farmers remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field and industry standards, it would have prevented the intrusions into their systems and, ultimately, the theft of PI.

64. As a direct and proximate result of Farmers' actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take time which they otherwise would have dedicated to other life demands, such as work and family, in an effort to mitigate the actual and potential impact of the Unauthorized Data Disclosure on their lives.

65. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[26]

[26] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited May 29, 2021).

66. As a result of Farmers' failures to prevent the Unauthorized Data Disclosure, Plaintiff and Class Members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft, and/or unauthorized use of their PI,

b. Out–of–pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud,

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Unauthorized Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud,

d. The continued risk to PI in Defendants' possession, which remains accessible to Defendants and is subject to further breaches so long as Farmers fails to undertake appropriate measures to protect the PI in their possession; and

e. Current and future costs in terms of time, effort, and money needing to be expended to prevent, detect, contest, remediate, and repair the impact of the Unauthorized Data Disclosure for the remainder of the lives of Plaintiff and Class Members.

67. In addition to a remedy for the economic harm, Plaintiff and the Class Members maintain an undeniable interest in ensuring their PI is secure, remains private, and is not subject to further misappropriation and theft.

68. To date, other than providing 12–months of credit monitoring and answering fraud related questions, Farmers does not appear to be taking any measures to assist Plaintiff and Class Members, other than simply telling them to:

- "Order your free credit report"
- "Place a fraud alert on your credit bureau file"

- "Place a security freeze on your credit file"
- "Report suspicious activity"

None of these recommendations, however, require Farmers to expend any effort to protect Plaintiff's and Class Members' PI. It is also not clear that Farmers has made any determination that the credit monitoring and identity protection services are designed or adequate to ameliorate the specific harms of having an exposed driver's license number.

69. Farmers' failure to adequately protect Plaintiff's and Class Members' PI shifts the burden onto Plaintiff and Class Members to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money. Instead, as Farmers' notice indicates, it is putting the burden on Plaintiff and Class Members to discover possible fraudulent activity and identity theft.

70. Farmers' offer of 12–months of identity monitoring and identity protection services to Plaintiff and Class Members is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when PI is acquired and when it is used.

G. Farmers' delay in identifying and reporting the breach caused additional harm.

71. The actual date Plaintiff and the Class Members' PI was improperly exposed is currently unknown to Plaintiff. However, Farmers discovered the Unauthorized Data Disclosure on or about February 12, 2021, and it was not until over two months later, in or about April 22, 2021, that Farmers began notifying those affected by the Unauthorized Data Disclosure—depriving Plaintiff and Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Unauthorized Data Disclosure.

72. As a result of Farmers' delay in detecting and notifying Plaintiff and Class Members of the Unauthorized Data Disclosure, the risk of fraud for Plaintiff and Class Members has been driven even higher.

CLASS ACTION ALLEGATIONS

73. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of himself and the following proposed Nationwide Class, defined as follows:

> All persons in the United States whose PI was compromised in the Unauthorized Data Disclosure announced by Farmers on or near April 22, 2021.

74. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff also brings this action on behalf of himself and the following proposed New York Subclass Class, defined as follows:

> All persons in the state of New York whose PI was compromised in the Unauthorized Data Disclosure announced by Farmers on or near April 22, 2021.

75. The Nationwide Class and New York Subclass will be referred to collectively as "the Class" except where necessary to distinguish between them.

76. Excluded from the proposed Class are any officers or directors of Defendants; any officers or directors of any affiliates, parents, or agents of Farmers; anyone employed by counsel in this action; and any judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

77. **Numerosity.** Members of the proposed Class likely number in at least the tens of thousands and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendants' own records.

78. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

a. Whether Defendants engaged in the wrongful conduct alleged herein,

b. Whether Defendants' inadequate data security measures were a cause of the Unauthorized Data Disclosure,

c. Whether Defendants owed a legal duty to Plaintiff and the other Class Members to exercise due care in collecting, storing, and safeguarding their PI,

d. Whether Defendants negligently or recklessly breached legal duties owed to Plaintiff and the other Class Members to exercise due care in collecting, storing, and safeguarding their PI,

e. Whether Defendants' online quote system auto-populated prospective quotes with PI obtained from the records of Defendants or third parties without the permission or consent of Plaintiff and the Class,

f. Whether Plaintiff and the Class are at an increased risk for identity theft because of the data security breach,

g. Whether Defendants violated the Drivers' Privacy Protection Act, 18 U.S.C. § 2724,

h. Whether Plaintiff and the Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief, and

i. Whether Plaintiff and the Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

79. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

80. **Typicality:** Plaintiff's claims are typical of the claims of the Members of the Class. All Class Members were subject to the Unauthorized Data Disclosure and

had their PI accessed by, used and/or disclosed to unauthorized third parties. Defendants' misconduct impacted all Class Members in the same manner.

81. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the other Class Members he seeks to represent; he has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

82. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class Members to individually seek redress for Defendants' wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION

Violation of the Drivers' Privacy Protection Act ("DPPA"), 18 U.S.C. § 2724

(On behalf of Plaintiff and the Nationwide Class)

83. Plaintiff incorporates the above allegations by reference.

84. The DPPA provides that "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted

under this chapter shall be liable to the individual to whom the information pertains." (18 U.S.C. § 2724.)

85. Under the DPPA, a "'motor vehicle record' means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles.'" (18 U.S.C. § 2725(a).) And the DPPA's definition of "personal information" includes an individual's driver identification number, commonly referred to as a driver's license number. (18 U.S.C. § 2725(3).) Therefore drivers' license numbers that are maintained as a part of a database of DMV records are motor vehicle records, and part of the personal information intended to be protected under the DPPA.[27][28]

86. Defendants also obtain motor vehicle records directly from state agencies or through resellers who sell such records, and also from their customers. During the time period up until and including at least February 12, 2021, PI, including drivers' license numbers, of Plaintiff and Class Members, were publicly available on Farmers' instant quote webpage and Farmers knowingly both used and disclosed Plaintiff's and members of the class's motor vehicle records for a purpose not permitted by the DPPA pursuant to 18 U.S.C. §§ 2724 and 2721(b).

87. Because of Defendants' violations of the DPPA, Plaintiff and putative Class Members are entitled to actual damages, liquidated damages, punitive damages, attorneys' fees and costs.

---

[27] "Personal information is 'from' a motor vehicle record when it derives from state DMV sources." (*Pub. Int. Legal Found. v. Boockvar*, 431 F. Supp. 3d 553, 562 (M.D. Pa. 2019), citing *Dahlstrom v. Sun-Times Media, LLC*, 777 F.3d 937, 949 (7th Cir. 2015); *Whitaker v. Appriss, Inc.*, No. 3:13-CV-826, 2014 WL 4536559, at *3 (N.D. Ind. Sept. 11, 2014) (citation omitted); *Andrews v. Sirius XM Radio Inc.*, 932 F.3d 1253, 1260 n.5 (9th Cir. 2019); *Siegler v. Best Buy Co. of Minn.*, 519 F. App'x 604, 605 (11th Cir. 2013)). It is irrelevant that the information does not take the form of a "motor vehicle record," and the DPPA protects "information" held by the DMV and supplied in connection with a motor vehicle record. (*Id.*; *see* 18 U.S.C. § 2721.)

[28] DPPA applies to personal information acquired from a state DMV. (*Hatch v. Demayo*, No. 1:16CV925, 2021 WL 231245, at *6 (M.D.N.C. Jan. 22, 2021).)

SECOND CAUSE OF ACTION

Negligence

(On behalf of Plaintiff and the Nationwide Class)

88. Plaintiff incorporates the above allegations by reference.

89. Defendants owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff's and Class Members' PI from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, implementing, maintaining, and testing their data security systems to ensure that Plaintiff's and Class Members' PI in Defendants' possession, or that could be accessed by Defendants, was adequately secured and protected.

90. Defendants owed a duty of care to Plaintiff and Members of the Class to provide security, consistent with industry standards, to ensure that their systems and networks adequately protected PI Defendants stored, maintained, and/or obtained.

91. Defendants owed a duty of care to Plaintiff and Members of the Class because they were foreseeable and probable victims of any inadequate data security practices. Defendants knew or should have known of the inherent risks in having their systems auto–populate online quote requests with private PI without the consent or authorization of the person whose PI was being provided.

92. Unbeknownst to Plaintiff and Members of the Class, they were entrusting Defendants with their PI when Defendants obtained their PI—including but not limited to their driver's license numbers—from motor vehicle department records and other businesses. Defendants had an obligation to safeguard their information and was in a position to protect against the harm suffered by Plaintiff and Members of the Class as a result of the Unauthorized Data Disclosure.

93. Defendants' own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their PI. Defendants' misconduct included failing

to implement the systems, policies, and procedures necessary to prevent the Unauthorized Data Disclosure.

94. Defendants knew, or should have known, of the risks inherent in collecting and storing PI and the importance of adequate security. Defendants knew about—or should have been aware of—numerous, well-publicized unauthorized data disclosures affecting businesses, especially insurance and financial businesses, in the United States.

95. Defendants knew and published an article acknowledging the importance of computer security and promoting the use of penetration in June 2019—a year and half before the Data Breach.[29]

96. Defendants breached their duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security to safeguard the PI of Plaintiff and Class Members.

97. Because Defendants knew that a breach of their systems would damage thousands of individuals whose PI was inexplicably stored or was accessible, including Plaintiff and Class Members, Defendants had a duty to adequately protect their data systems and the PI contained and/or accessible therein.

98. Defendants also had independent duties under state and federal laws requiring Defendants to reasonably safeguard Plaintiff's and Class Members' PI.

99. Defendants' alleged negligent acts and omissions permitted unauthorized individuals access to Defendants' systems that stored and/or accessed Plaintiff's and Class Members' PI, which violates Section 5 of the FTC Act prohibiting "unfair . . . practices in or affecting commerce." This includes failing to have adequate data security measures and failing to protect Plaintiff's and the Class Members' PI.

100. Plaintiff and the Class Members are among the class of persons Section 5 of the FTC was designed to protect, and the injuries suffered by Plaintiff and the

[29] https://www.farmers.com/learn/plan-and-prep/phishing-scams-and-other-high-tech-mischief/ (Last visited August 20, 2021.)

Class Members are the types of injury Section 5 of the FTC Act was intended to prevent.

101. Neither Plaintiff nor the other Class Members contributed to the Unauthorized Data Disclosure as described in this Complaint.

102. As a direct and proximate cause of Defendants' conduct, Plaintiff and Class Members have suffered and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PI is used; (ii) the publication and/or theft of their PI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PI; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Unauthorized Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PI, which remains in Defendants' possession (and/or Defendants have access to) and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PI in their continued possession; and, (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PI.

THIRD CAUSE OF ACTION

Declaratory and Injunctive Relief

(Brought by Plaintiff and the Nationwide Class)

103. Plaintiff incorporates the above allegations by reference.

104. This Count is brought under the federal Declaratory Judgement Act, 28 U.S.C. §2201.

105. As previously alleged, Plaintiff and Class Members had a reasonable expectation that companies, such as Defendants, who could access their PI through automated systems, would provide adequate security for that PI.

106. Defendants owe a duty of care to Plaintiff and Class Members, requiring Defendants to adequately secure Plaintiff's and Class Members' PI.

107. Defendants still possesses Plaintiff's and Class Members' PI.

108. Since the Unauthorized Data Disclosure, Defendants have announced few, if any, changes to their data security infrastructure, processes, or procedures to fix the vulnerabilities in their computer systems and/or security practices that permitted the Unauthorized Data Disclosure to occur and, thereby, prevent further attacks.

109. The Unauthorized Data Disclosure caused actual harm because of Defendants' failure to fulfill their duties of care to provide adequate security measures to Plaintiff's and Class Members' PI. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PI and Defendants' failure to address their security failings that lead to the Unauthorized Data Disclosure.

110. Defendants' failure to meet their legal duties of care is ongoing because there is no reason to believe Defendants' security measures are any more adequate now than they were before the Unauthorized Data Disclosure.

111. Plaintiff, therefore, seeks a declaration that (1) Defendants' existing security measures do not comply with their duties of care to provide adequate security, and (2) Defendants must implement and maintain reasonable security measures to comply with their duties of care, including, but not limited to:

a. Ordering Defendants to engage third–party security auditors/penetration testers, as well as internal security personnel, to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and

ordering Defendants to promptly correct any problems or issues detected by such third–party security auditors;

b. Ordering Defendants to engage third–party security auditors and internal personnel to run automated security monitoring;

c. Ordering Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

d. Ordering Defendants not to transmit PI via unencrypted email and not to put PI as part of their source code or otherwise make PI available on their instant quote webpage;

e. Ordering Defendants not to store PI in email accounts or in any publicly facing website;

f. Ordering Defendants to purge, delete, and destroy, in a reasonably secure manner, customer data not necessary for its provisions of services;

g. Ordering Defendants to conduct regular computer system scanning and security checks; and

h. Ordering Defendants to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a disclosure when it occurs and what to do in response to a breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all others similarly situated, respectfully requests the Court enter an order:

a. Certifying the proposed Class as requested herein,

b. Appointing Plaintiff as Class Representative and undersigned counsel as Class Counsel,

c. Finding Defendants engaged in the unlawful conduct as alleged herein,

d. Granting injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business, in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members'

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' personal information;

v. prohibiting Defendants from maintaining Plaintiff's and Class Members' personal information on a cloud–based database and/or server;

vi. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

vii. requiring Defendants to conduct regular database scanning and security checks;

viii. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling

personal information, as well as protecting Plaintiff's and Class Members' personal information;

ix. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal information;

x. requiring Farmers to meaningfully educate Plaintiff and Class Members about the threats they face as a result of the loss of their confidential personal information to third parties, as well as the steps Plaintiff and Class Members must take to protect themselves;

xi. requiring Defendants to design, maintain, and test their computer systems to ensure PI in their possession is adequately secured and protected;

xii. requiring Defendants disclose any future data disclosures in a timely and accurate manner;

xiii. requiring Defendants to implement multi–factor authentication requirements; and

xiv. requiring Defendants to provide lifetime credit monitoring and identity theft repair services to Plaintiff and Class Members.

e. Awarding Plaintiff and Class Members damages;

f. Awarding Plaintiff and Class Members pre–judgment and post–judgment interest on all amounts awarded;

g. Awarding Plaintiff and Class Members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the proposed Class, hereby demand a trial by jury as to all matters so triable.

Dated: September 8, 2021

/s/ Michael Kind
Michael Kind

Michael Kind
Mk@kindlaw.com
Kind Law Firm
8860 S. Maryland Parkway, Suite 106
Las Vegas, NV 89123
(702) 337-2322

Gayle M. Blatt* (CA 122048)
gmb@cglaw.com
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232

Kate M. Baxter-Kauf* (MN #0392037)
Kmbaxter-kauf@locklaw.com
Karen Hanson Riebel* (MN #0219770)
khriebel@locklaw.com
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981

*(*pro hac vice forthcoming)*

Attorneys for Plaintiff and the putative Class